Sussex Research Online

The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges

Article (Published Version)

Bu, Qingxiu (2021) The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. International Cybersecurity Law Review, 2. pp. 113-145. ISSN 2662-9720

This version is available from Sussex Research Online: http://sro.sussex.ac.uk/id/eprint/100151/

This document is made available in accordance with publisher policies and may differ from the published version or from the version of record. If you wish to cite this item you are advised to consult the publisher's version. Please see the URL above for details on accessing the published version.

Copyright and reuse:
Sussex Research Online is a digital repository of the research output of the University.

Copyright and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable, the material made available in SRO has been checked for eligibility before being made available.

Copies of full text items generally can be reproduced, displayed or performed and given to third parties in any format or medium for personal research or study, educational, or not-for-profit purposes without prior permission or charge, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

http://sro.sussex.ac.uk

Int. Cybersecur. Law Rev. (2021) 2:113–145
https://doi.org/10.1365/s43439-021-00022-x

ORIGINAL PAPER

The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges

Qingxiu Bu

Received: 13 February 2021 / Accepted: 9 March 2021 / Published online: 7 April 2021
© The Author(s) 2021

Abstract The digital revolution transforms people's view about values and priorities. Automated facial recognition (AFR) comes with many concerns as well as benefits. The technology raises significant legal and ethical challenges, which risk perpetuating systemic injustice unless countervailing measures are put in place. The way facial images are obtained and used, potentially without consent or opportunities to opt out, can have a negative impact on people's privacy. Laws on privacy vary across jurisdictions, which has an enormous effect on measures that could be taken to safeguard AFR-related ethical concerns. In an era of digitalisation, the existing laws are ill-equipped to address evolving needs against threats to individual privacy. Integrating the principles of proportionality and necessity, of the upmost importance is to ensure the proper use of AFR in a socially responsible way. It is imperative to build an AFR infrastructure that incorporates society's legal and ethical commitments, and further address the challenges of governing the technology.

Keywords Social license · Consent · Digital · Algorithm · Biometric

1 Introduction

Technological advances in the form of image analysis and algorithmic processing have generated a significant change in the capability of facial recognition. Automated facial recognition (AFR) is a biometric technology that uses cameras to match live footage of individuals with images from a database [1]. As a computer-based security system, it helps to verify the identity of a person based on the individual's

Q. Bu (✉)
Chair of Global Law Initiative, Sussex Law School, University of Sussex, Freeman Centre, F20, BN1 9QE, Falmer, UK
E-Mail: Q.Bu@sussex.ac.uk

biometric data. AFR is rapidly being deployed by private actors as well as law enforcement agencies, permeating nearly every aspect of the society. Given its dual use in nature, AFR can be used for beneficial or malicious purposes. The technology has sparked an intense debate on its potential impact on fundamental rights, of which the protection of privacy is at the core. Despite its widespread use, AFR is operating in a legal grey area. The risk-intensive processes of AFR shed light on the limits of current legal and ethical frameworks, which entails a global challenge to alleviate the impending threats to privacy. This article seeks to explore potential legal and regulatory approaches in selected jurisdictions and address these challenges from multipronged perspectives.

This article proceeds as follows: Part I starts with a benefit–cost analysis and further ascertains whether the use of AFR is viable or untenable in terms of privacy protection. Part II looks at privacy provisions under the General Data Protection Regulation (GDPR) and a ruling by the European Court of Human Rights (ECtHR) that exemplifies how privacy is therein protected. Part III discusses the latest U.S. statutory approaches to the AFR-driven challenges. Some cases are reflective of the laws' application at both state and federal levels. Part IV compares the UK and China's efforts in governing the AFR-related practice respectively by the policy and a private entity. It is indicated that neither country is equipped with adequate governance regimes. Arguably, there is little difference of current approaches between each other, despite the plausibly considerable divergences between the two legal systems. Part V refers to a social license theory that involves AFR's social acceptability. It presents how AFR plays its role when privacy implications arise. Although a public private partnership (PPP) could improve the AFR's performance, further measures, such as impact assessments, need to be embedded into practice by both public and private actors. Part VI puts forward a paradoxical game theory in surveillance and date collection and seeks to address ethical and legal challenges. This part casts a challenge on a long-standing theory of moral and ethical supremacy and inferiority in the context of AFR deployment. With the intense competition for AI supremacy, the divergences are narrowed down, and lines blurred between the West and China. Part VII analyses principles of necessity and proportionality to ensure that the AFR system meets relevant legal requirements. Some proposals are provided in furtherance of the debate on AFR's global governance with particular regard to its safeguard infrastructure and institutions. The concluding remark affirms a momentous duty for both public and private actors to get the most out of AFR while still protecting privacy. With the balance highlighted between privacy protection and crime deterrence, further research needs to be undertaken given the lack of more critical qualitative and quantitative data analysis. The pressing inquiries can only be addressed from a multifaceted perspective.

2 AFR's benefits and privacy challenges

As a dual-use technology, AFR has a wide range of benefits and potential privacy implications. It can be used for well-intended purposes that have serious social consequences [2]. One should take account of AFR's potential cost while benefiting

from the use of the tool. AFR, if used properly, can enhance law enforcement capabilities and protect public safety. However, its detrimental effects should not be ignored, since the intrusive technology could destroy people's privacy rights and force them to change their behaviour.

2.1 Benefits

AFR has the potential to bring about enormous benefits, such as crime prevention and counterterrorism [3]. It deters terrorism through analysing past crimes to predict the chances that criminals will reoffend. The technology helps to create reliable evidence from video footage and keep track of criminals and potential law-breakers, enabling law enforcement to react effectively [4, 5]. Given its "sense-enhancing" function, AFR enables enforcement agencies to do more than ordinary surveillance [5] and can aggregate and assess vast quantities of data that are beyond human capacity to analyse unaided [6]. It shows that "facial recognition software got twenty times better at searching a database to find a matching photograph", which is based on evaluations of 127 algorithms from 39 developers that have been undertaken between 2014 and 2018 [7]. These algorithms can work more accurately than can their human counterparts. Thus, AFR improves efficiency of law enforcement and enhances a state's national security. Private actors employ AFR for commercial profits as well. Even if these benefits sound appealing, there are many unexpected privacy concerns associated with the use of the tool [8].

2.2 Privacy: a cornerstone for the enjoyment of fundamental rights

Privacy is a core value inherent to a liberal democratic and pluralist society, and a cornerstone for the enjoyment of fundamental rights [9]. Given a high degree of intrusion into privacy, AFR is considered as more concerning than other biometric techniques [10]. Once stored, data are difficult to completely delete, leading to the so-called "data persistence" [11]. Privacy is challenged when anyone's online searches can recognise a person across vast sets of facial data in real time [12]. First of all, privacy is not an abstract concept, but a contextual one. A reasonable expectation of privacy refers to the extent to which people can expect privacy in public spaces without being subjected to surveillance [11]. AFR deployment in a particular context may violate such reasonable expectations [13]. The threat of perpetual surveillance erodes fundamental rights, because there is a significant gap between the AFR and the laws regulating its use [4]. Secondly, it is not to an absolute but a qualified right, which inherently allows for the permissible restriction of the protection to arbitrary or unlawful interference [14]. Even the attainment of privacy could be subject to limitations; values are modulated by circumstances with AFR being used circumstantially in both private and public spheres [15]. It is more sensible to explore whether AFR uses can be justified by the needs of the surrounding context. It might be less critical particularly if other important values are at stake. However, any interference needs to be adequately justified [16] and cannot compromise the essential, inalienable core of the right [17]. AFR should

operate in an adaptive manner to ensure that the digital world has places where law-abiding people can enjoy privacy [18].

2.3 Is an outright ban a panacea?

AFR presents far too serious a threat to privacy interests, and triggers many debates on the parameters of privacy [5]. For instance, the storage of facial measurements in code makes people's facial identity easy to transpose. As such, the question arises as to whether the use of AFR should be banned until the right legal framework along with privacy and security safeguards are in place [19, 20]. Arguably, a blanket ban on AFR is not the answer to the concerns, which, otherwise, would deny consumers the convenience that AFR entails. As discussed above, AFR creates innovative benefits for society and should continue to be developed. The central concern is that the deployment of AFR needs to be adequately regulated to preserve privacy. Precision regulation would make up for the gap where there is greater risk of societal harm [21]. However, it takes time to enact new laws and relevant guidance on trial protocols.

3 Provisions under the general data protection regulation (GDPR)

EU data protection rules clearly cover the processing of biometric data. Under the EU law, biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images".[1] Facial images constitute biometric data, as they can be used to identify individuals. The EU protects people from the threats of facial recognition by enforcing the General Data Protection Regulation (GDPR), which prevents the processing and sharing of biometric data without consent.

3.1 Applying the GDPR in the deployment of AFR

The GDPR generally forbids the processing of biometric data for uniquely identifying purposes unless one can rely on one of the 10 exemptions.[2] The law provides that collection and processing of biometric data including facial recognition is valid when "the data subject has given explicit consent to the processing of personal data".[3] The national and EU legislators have the discretion to decide the cases where the use of this technology guarantees a proportionate and necessary interference with human rights.[4] The GDPR shows the beginning of resistance to untrammelled data collection. It requires that organisations collect and process data only with the clear and informed consent of individuals. Notably, the use of AFR by law enforcement

[1] Law Enforcement Directive, Art. 3 (13); GDPR, Art. 4 (14); Regulation (EU) 2018/1725, Art. 3 (18).

[2] GDPR Art. 9 (2).

[3] GDPR Art. 9(2)(a).

[4] GDPR Art. 9(2) (g).

agencies is not subject to the GDPR, but the Law Enforcement Directive (LED).[5] The most relevant instrument establishes a comprehensive system of personal data protection. The LED specifically refers to facial images as 'biometric data' when used for biometric matching for the purposes of the unique identification of a natural person.[6] Pursuant to the European model, law enforcement may not engage in a particular investigative method until it has been fully authorised by statute [22].

3.2 Exemptions under the GDPR

The GDPR includes exemptions for the collection of biometric data like facial recognition by authorities, even though such information is considered "sensitive" and highly restricted in the hands of private companies. Regarding the applicability of Article 8 of the European Convention of Human Rights (ECHR) on the right to respect for private life, a government may interfere with these rights if sufficiently justified by legality and necessity. It requires that personal data be processed only for specified purposes, which must be explicitly defined by law. Such purposes need to be "specified, explicit and legitimate" and transparently communicated to the data subject.[7] It is essential to examine exceptional circumstances from perspectives of proportionality, necessity and the balancing of interests. A three-pronged test developed by the ECtHR requires that:

> Any rights interference has to pursue a legitimate aim; be in accordance with the law, i.e. necessitating an appropriate legal basis meeting qualitative requirement,[8] as well as necessary in a democratic society.[9]

These principles will be discussed in more detail in the seventh part of this article. In judicial practice, courts are increasingly siding with people's rights and limiting the use of privacy-invading policing tactics like AFR surveillance, as legal challenges arise against the use of mass surveillance [23]. The ECtHR also found in *Peck v. the United Kingdom* that video surveillance of public places where the visual data is recorded, stored and disclosed to the public fell within the scope of Article 8.[10] The ECtHR has ruled that UK laws enabling mass surveillance had violated human rights,[11] and more specifically the right to privacy protected by Article 8 of the ECHR.[12]

As the most prominent legislative act related to AFR, the GDPR raises questions about the legality of the new storage regimes and mechanisms for transfer of bio-

[5] EU Data Protection Directive 2016/680.

[6] Law Enforcement Directive, Art. 3 (13).

[7] GDPR Art. 34; The UK Data Protection Act (DPA 2018) s15.

[8] *Gorlov and Others v. Russia* (Nos. 27057/06, 56443/09 and 25147/14, ECtHR, 2 July 2019) §97.

[9] *S. and Marper v. the United Kingdom* (Nos. 30562/04 and 30566/04, ECtHR Grand Chamber 4 December 2008) §§ 95–104.

[10] *Peck v. United Kingdom*, App No 44647/98, ECHR 2003-I, [2003] ECHR 44, (2003) 36 EHRR 41, (2003) 36 EHRR 719.

[11] *Big Brother Watch & Others v. The United Kingdom* (ECtHR, 13 September 2018) §387.

[12] *Big Brother Watch & Others v. The United Kingdom* (ECtHR, 13 September 2018) §251.

metric data. Many social challenges presented by AFR are not wholly addressed via the GDPR. This is attributed largely to low evolution in updating conceptual and theoretical challenges. The European Commission is planning to impose stricter limits on facial recognition usage to give EU citizens explicit rights over the use of their facial data [24]. It seems that the EU does not censor online content, nor does it grant law enforcement agencies access to personal data without a court order.

4 AFR-related laws in the U.S.

Law enforcement in face recognition affects over 117 million American adults, who have been captured in a "virtual, perpetual lineup" [25]. Like the EU, the U.S. takes a similar stance against AFR-related violations of privacy, which is reflected not only in its statutory but also some high-profile precedents. Although the U.S. has so far opted for minimal regulation, the statutory approaches have far-reaching implications given the enactment of AFR-specific laws at both state and federal levels.

4.1 Precedents related to emerging technologies and privacy

The Court has been concerned about systems of digital surveillance and their potential privacy invading power [26]. In *Katz v. United States*, the Supreme Court adopted a two-part test to determine whether a person has a reasonable expectation of privacy, assessing:

(i) Whether the person exhibited an actual, subjective expectation of privacy
(ii) Whether that expectation is one that society recognises as reasonable.[13]

The *Katz* test provides a framework for analysing Fourth Amendment issues. In *United States v. Jones*, Justice Sonia Sotomayo concurred that the court's jurisprudence might not be adequate in "cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property".[14] Justice Alito highlighted the need to enact new law that:

> In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative … to balance privacy and public safety in a comprehensive way.[15]

In *Carpenter v. United States*, the Supreme Court held that the government's warrantless access to an extensive compilation of cell phone user data violated the Fourth Amendment.[16] However, the Court declined to address whether short-term, limited or real-time access had equal concerns under the Fourth Amendment.[17] A

[13] *Katz v. United States* 389 U.S. 347 (1967).

[14] *Jones v. United States* 565 U.S. 400 (2012).

[15] *United States v. Jones*, 565 U.S. 400, 429–30 (2012) (Alito, J. concurring).

[16] *Carpenter v. United States* 138 S. Ct. (2018) at 2219.

[17] *Carpenter v. United States* 138 S. Ct. (2018) at 2220

fundamental question embedded in the above three cases is whether the surveillance system being used leads to a violation of a reasonable expectation of privacy.

There is a circuit split on the extent to which plaintiffs must show harm in order to bring privacy and data breach causes of action [27]. The Supreme Court in *Spokeo v. Robins* held that: "a statutory violation is not in itself sufficient to create standing if the injuries are not concrete".[18] As Ohm noted, the Court is concerned with systems of digital surveillance from the Supreme Court's analytical perspectives, like depth, scope and breadth [28]. In *Facebook v. Patel*, it was alleged that Facebook misled tens of millions of users about their ability to control facial recognition within their accounts.[19] The privacy-protective case helps frame the analysis, and the ruling in *Facebook v. Patel* would have shaped how courts view AFR. However, the Supreme Court declined to hear the case. Although, in *Riley v. United States,* the Supreme Court's quantitative and qualitative analysis applies to the challenges of AFR surveillance,[20] there has so far been no developed case law or constitutional precedent upholding the police use of facial recognition without a warrant. The court has not even decided whether facial recognition constitutes a search under the Fourth Amendment. Critics have argued that AFR may implicate the First Amendment right to privacy.

4.2 Statutory approaches to addressing AFR's implication of privacy

The California Consumer Privacy Act (CCPA 2019) is likely to set the legal hurdle high for businesses deploying the technology.[21] The latest legislation to limit AFR is referred to as the Body Camera Accountability Act.[22] The Californian City of San Francisco hereby bans AFR because of its excessively intrusive nature into people's privacy and to avoid possible abuse by law enforcement agencies [29–31]. CCPA 2019 has substantial impact on privacy rights and consumer protection, which is sometimes considered as a model for a federal data privacy law. On 14 March 2019, the Commercial Facial Recognition Privacy Act (CFRPA) was introduced by senators to offer legislative oversight on AFR's commercial application [32]. CFRPA 2019 prohibits the use of AFR in the absence of affirmative consent from a data subject [33]. It seeks legal changes that require companies to inform before facial recognition data is acquired. The law sets general limits on which information businesses can collect from individuals, and what can be done with it. The legislations represent an important step toward protecting privacy. They are conducive to strengthening consumer protections by prohibiting commercial users of AFR from collecting and re-sharing data for identifying or tracking consumers without their consent.

[18] *Spokeo, Inc. v. Robins* 136 S. Ct. 1540 (2016).

[19] *Patel v. Facebook, Inc.,* 932 F.3d 1264, 1273 (9th Cir. 2019).

[20] *Riley v. United States* 134 S. Ct. 2473, 2480 (2014).

[21] Cal. Legis. Serv. Ch. 579 (A.B. 1215). The CCPA was passed in June 2018 and effective as of 1 January 2020.

[22] Body Camera Accountability Act (AB 1215) Approved by Governor 8 October 2019. Filed with Secretary of State on the same day.

5 Legal challenges against the use of AFR in the UK and China

The use of AFR for policing purposes has in recent years emerged as an acute controversy. Some debates are initiated amongst privacy issues versus protecting the public. Not only is AFR routinely used by law enforcement agencies, but also by private actors. There is no legislation specifically designed to regulate the use of AFR. Underlining the controversial nature of AFR, the use has brought legal challenges in both China and the UK. With AFR integrated into China's rapidly expanding networks of surveillance, a claimant accused a wildlife park of compulsorily collecting visitors' biometric data via facial recognition. The UK is also one of the most surveilled countries in the world [34], where a plaintiff's challenge against policy is on the grounds that the use of AFR breaches the right to privacy and data protection laws. Both cases' legal bases have been called into question.

5.1 R (Bridges) v. CCSWP and SSHD

AFR has the potential to become an epidemic of intrusiveness [35]. The technology presents obvious questions over whether police are violating citizens' privacy protections. A challenge to the South Wales Police's use of AFR on the basis of data protection and human rights infringements has been unsuccessful before the High Court of England and Wales, although the decision is still in the process of being appealed[23] [36]. At the heart of this case lies a dispute about the privacy and data protection implications of AFR. The tool involves the processing of sensitive personal data, which requires the users to comply with the Data Protection Act (DPA 2018). It remains uncertain whether the trials demonstrate full compliance with the law. In judgment, Lord Justice Haddon-Cave and Mr Justice Swift found that AFR did interfere with the right to private life under Article 8 of the ECHR. Nevertheless, Mr Justice Swift held that:

> ... South Wales police's use to date of AFR has been consistent with the requirements of the Human Rights Act and the data protection legislation.[24]

The court agreed that although AFR amounted to interference with privacy rights, there was a lawful basis for it and the legal framework used by the police was proportionate. The decision was considered as a green light for widespread deployment of AFR as a crime-fighting panacea [37].

The primary arguments before the Court of Appeal on 23 June 2020 are whether the Divisional Court erred in their analysis of the application of Article 8(2) and whether the legal framework governing the use of AFR has the requisite quality.[25] The judgment remains reserved. The case is significant not just for the ongoing use of AFR but for its future governance. It has profound implications for the way that society is policed. It is noteworthy that the judgment itself considers solely the use of AFR by the police rather than any other public or private bodies [38].

[23] *R (Bridges) v. CCSWP and SSHD* [2019] EWHC 2341 (Admin).

[24] *R v. The Chief Constable of South Wales Police and SSHD* [2019] EWHC 2341(Admin).

[25] *R (Bridges) v. Chief Constable of South Wales Police* [2020] 1 WLR 672.

The current legislative and regulatory framework on AFR use is insufficient. The real-time facial recognition cameras are biometric checkpoints, identifying members of the public without their knowledge [39]. There is neither a regulatory framework limiting the AFR's law enforcement applications, nor legislation regulating its use by private actors for commercial purposes. The legal framework which currently applies to the use of AFR by law agencies and private actors does not ensure those rights are sufficiently protected. Apparently, AFR has profound consequences for privacy and data protection rights. The lack of legislation surrounding the use of AFR has called into question the legal basis of the trials [40].

In *RMC and FJ v. MPS*, the court found that the "indefinite retention of the claimant's [custody photographs] was an unjustified interference with their rights" under Article 8 of the ECHR.[26] The High Court ruling indicates that retaining the custody images of unconvicted people amounted to a breach of human rights, as the court realised that: "the algorithms of the law must keep pace with new and emerging technologies".[27] The *Bridges* litigation is the first case of its kind around the world and will likely be influential in the approach taken by jurists in this developing area of law across jurisdictions [41]. As Ruhrmann observed:

> Even in mature democracies with a strong commitment to protecting civil liberties, establishing policy safeguards for the use of AFR in law enforcement in accordance with human rights remains challenging [42].

Due to the absence of a legal basis and the risks inherent in AFR, it is vital to create a framework within which state agencies can work to ensure security and privacy.

It remains unanswered as to whether there should be a specific legal framework for the police and other actors to routinely deploy AFR, although the court held that the current national legal regime is adequate to ensure the appropriate use of AFR.[28] The DPA 2018 is the primary UK legislation controlling how personal data is used by the public and private sectors and contains extensive regulation of the processing and control of data [43]. Police deploying AFR must comply with the DPA 2018, and the Surveillance Camera Code of Practice [44]. Relevant to the retention of images for comparison against faces viewed through AFR is that DPA 2018 classifies "custody images" as personal data [48]. In addition, the Criminal Justice and Public Order Act (CJPOA 1994) confers on police the power to require removal of facial coverings in England and Wales if they feel they are being worn for the purpose of concealing identity and if they believe incidents involving violence may take place in any locality.[29] Furthermore, the Protection of Freedoms Act of 2012 only applies indirectly to the use of AFR by mandating a code of practice

[26] *RMC and FJ v. Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin).

[27] *R v. The Chief Constable of South Wales Police and SSHD* [2019] EWHC 2341(Admin).

[28] *Bridges v. Chief Constable of South Wales Police and others*, [2019] EWCH 2341 (Admin) 4 September 2019 §159.

[29] CJPOA 1994 s 94 (227).

for surveillance camera systems [45]. However, these legal regimes do not provide guidelines or rules specifically regulating the use of AFR by the police [46].

The UK government has not yet passed new regulations in this specific arena. The regulatory framework gives little indication or guidance about the proper threshold at which AFR can be lawfully used. Law normally lags behind technology, and AFR currently exists in a regulatory vacuum, so at present it is being used in ways that undermine public confidence in the systems they avail of [47]. Private entities can start using it without declaring the move publicly or notifying authorities [48]. As such, given the lack of a regime regulating the use of AFR and biometric tracking capabilities, legislation needs to be brought forward that seeks to govern current and future biometric technologies [49]. A statutory code of practice is needed to govern how the police should use this technology.

5.2 *Bing Guo v. Hangzhou Safari Park* (Hangzhou Fuyang District Court, China, 2019)

In a landmark ruling, a Chinese court ruled that it was illegal for an entity to collect consumers' facial biometric data without their consent. It is the first case to challenge the commercial use of AFR and was brought to Hangzhou Fuyang District People's Court in October 2019. Bing Guo sued Hangzhou Safari Park after being required by the Park to scan his face to gain entrance. Guo claimed that the biometric system infringes upon consumers' privacy rights and jeopardises consumers' safety if abused. He further alleged that the Park had violated China's consumer protection law. On 20 November 2020, the Hangzhou Court made a judgement, holding that the defendant breached the principle of necessity, while altering the contract unilaterally [50]. The defendant was ordered to compensate Guo ¥RMB1038 (£118). Nevertheless, the court did not confirm explicitly whether the defendant had infringed privacy, although the ruling was made in Guo's favour that the Park's behaviour was a breach of contract [51]. Nor did the court order the defendant to delete all his biometric information, i.e. facial and fingerprint data. As such, an entity should gain consent *ex ante*, and comply with the principles of "legality, legitimacy and necessity" when collecting personal information. The decision could help rein in what has been a Wild West of mass data collection for commercial purposes [52].

5.2.1 Increasing awareness of privacy protection

The *Guo* case has triggered a growing debate about privacy and abuse of personal data in an increasingly digitised society. Despite the nominal compensation, the high-profile case upended the notion that Chinese people do not care about privacy. As Chinese people become increasingly aware of their privacy rights, the concept of data privacy is gaining ground in China. They are increasingly concerned about how their data is being collected and used via AFR. During a recent survey, a main concern is that the respondents are worried about their biometric data to be unduly leaked. A total of 80% of respondents said they were concerned that the AFR system operators had lax safeguard measures [53]. In all, 74% said they would prefer to use traditional identification (ID) methods to AFR for the sake of verifying

their identity [54]. However, the survey also suggested that around 60–70% of Chinese citizens believed AFR made public places safer. It indicated a broad public willingness to surrender their privacy in exchange for the safety and convenience that AFR entails [55]. In comparison, approximate 65% of the UK interviewees showed their discomfort around police uses of AFR with regard to privacy, surveillance, consent and ethics[15]. Around specific intense debate over deployment of AFR for applications in security and law enforcement, the surveys indicated little difference in privacy awareness between the two nationals. Both countries' people seek to strike a balance between increased security and interferences with their privacy [9]. The survey indicates growing pushback against AFR in China. It is far from clear whether this rising discomfort will give way to policy changes [56]. The fundamental solutions will have to come from within.

5.2.2 Regulations

The Ministry of Science and Technology (MST) issued *Governance Principles for a New Generation of Artificial Intelligence (AI): Develop Responsible AI* on 17 June 2019, which encompasses a principle of respect for privacy.[30] In June 2019, the Office of the Cyberspace Administration (OCA), the highest administrative internet regulator of China, has issued "*Data Protection Regulatory Guideline*", in which the protection of personal biometric information is highlighted. It provides directions on how to collect and use customer data, effectively setting personal data protection standards in China [57]. As China's first major digital privacy guideline, the Personal Information Security Specification (PISS 2018) took effect on 1 May 2018. It lays out guidelines for consent and how personal data should be collected, used and shared.[31] Although Cyber Security Law (CSL 2017) is considered to be the most authoritative law protecting personal information, the Personal Information Security Specification (PISS) 2018 is the effective centrepiece of an emerging system around personal data [58]. Its 2020 version strengthens privacy protection and revises the "exceptions to soliciting consent"[32] and refinements for personal biometric information.[33] In particular, PISS 2020 provides that "Personal biometric information is a type of Personal Sensitive Information and includes facial recognition features, which may not be shared or transferred in principle."[34] Despite the lack of penalties and legally-binding effects, PISS serves as an important reference for enforcement agencies.

5.2.3 Existing legal framework

There is a fragmented legal and regulatory landscape of privacy and data protection laws. Under Article 253 of the Criminal Law of the People's Republic of

[30] MST, 'Governance Principles for a New Generation of Artificial Intelligence' Principle 4.

[31] PISS 2018 Articles 3.5, 3.6, 3.11, and 3.12.

[32] PISS 2020 Art. 3 (6).

[33] State Administration for Market Regulation (SAMR), 'Information Security Technology-Personal Information Security Specification (PISS)' (GB/T 35273-2020, effective on 1 October 2020).

[34] PISS 2020 Art. 9 (2) (i).

China (PRC), illegally selling or providing citizens' personal information is subject to criminal penalties.[35] The Supreme People's Court (SPC) and the Supreme People's Procuratorate (SPP) jointly issued the *Judicial Interpretation on Several Issues Concerning the Application of Law in Criminal Cases of Infringing on Personal Information.*[36] Being legally binding, the *Judicial Interpretation* specifies criminal penalties for misusing citizen's personal information. Even if the personal information were legally collected, in the absence of the consent from the relevant individuals, one cannot provide such personal information to any third party. Doing so would be criminally actionable under the PRC Criminal Law.[37] The General Provisions of the Civil Law (GPCL) of China stipulates that: "'natural persons' personal information shall be protected by law".[38] Taking effect on 1 June 2017, the China Cyber Security Law (CSL 2017) bans online service providers from collecting and selling citizens' personal information without consent.[39] The law imposes legal obligations on operators by stating the requirements for the collection, use and protection of personally identifiable information (PII), which includes biometric data [59]. The consent requirement is echoed in China's Consumer Protection Law (CPL 2019), which provides that consumers' personal information can only be collected for legitimate purposes with consent.[40] In terms of the legal basis, the defendant's use of AFR has not gained the plaintiff's consent, let alone proper safeguards. China's Personal Data Protection Law (PDPL 2020) leads to a more comprehensive framework for individual data rights and protection, of which Article 16 highlights the compulsory consent. More importantly, PDPL 2020 has a strong focus on biometric data protection to curb facial recognition abuses.[41] The latest PRC Civil Code 2020 provides that an individual's biometric data is protected.[42] A victim could refer to this provision for remedies, despite the lack of specific narrative of AFR issues. As such, Guo could have sued the Park for the unauthorised use of his biometric data,[43] in lieu of claiming for the defendant's breach of the contract. Notably, there are currently neither laws governing the specific use of AFR, nor overarching principles of data protection being set at the national level. The legal and regulatory efforts mark a major step in China's tentative progress towards protecting Chinese citizens' personal data, although the law continues to evolve in this scenario.

[35] China Criminal Law Art. 253 (1).

[36] Supreme People's Court (SPC) and the Supreme People's Procuratorate (SPP), 'Judicial Interpretation on Several Issues Concerning the Application of Law in Criminal Cases of Infringing on Personal Information' was promulgated on 8 May 2018 and came into effect on 1 June 2018.

[37] PRC Criminal Law Art. 253 (1).

[38] General Provisions of the Civil Law (CPCL) Art.111.

[39] China Cyber Security Law 2017 Articles 41 & 42.

[40] China Consumer Protection Law 2019 Art. 29.

[41] PDPL 2020 Art. 3.

[42] PRC Civil Code 2021 Art. 1034.

[43] PRC Civil Code 2021 Art. 1035.

5.3 Far-reaching implications in both the UK and China

The cases have been the first of their kind respectively in China and the UK amid increasing concerns over indiscriminate use of AFR, due largely to the development of AFR outpacing legal safeguards. They are bound to have wide-reaching implications over the use of AFR by businesses as well as law enforcement agencies. The cases trigger a heated debate on the legitimacy and morality of adopting AFR [60]. Chinese people in general are far less suspicious of AFR and consider it as a positive way to bring convenience. Despite growing attention to the issue, China's personal data protection system is still made up of a patchwork of laws and standards in which users of AFR lack clear guidance [61]. Relevant laws and regulations are scattered, unsystematic and can barely provide effective or substantial legal protection for privacy. Legislators are generally not good at predicting future problems. It is a system that is short of adequate checks, balances and disclosure requirements, which should regularly be part of the western Europe or U.S. surveillance networks [62]. Nevertheless, there is a global rise in authoritarianism. Even in countries with strong rule of law traditions, AFR gives rise to legal and ethical challenges. In *Bridges*, police and intelligence agencies were using the same surveillance tools to solve and deter crimes and prevent terrorism. Notably, the judgement does not relate to AFR use by the private sector.

Any rules should be based on "notice and consent" when AFR is used to verify someone's identity. Problematically, the two countries enrol images without the data subject's active consent. Neither the law enforcement agencies in the UK nor the Chinese private actors have obtained the plaintiffs' consent before deploying AFR. In this vein, the two countries share a lot in common. Whether used by governments or private entities, AFR appears to be developing faster than the law and the government's ability to ensure its responsible use [63]. The proper use of provision and regulation of biometrics is key to ensuring that the criminal justice system functions effectively. Otherwise, AFR could result in miscarriages of justice [20]. The regulatory lacuna surrounding the use of AFR has called into question the legal basis of the trials [20]. Neither country has specific law to protect citizens' biometrics, which highlights a lack of a safeguards system. Legislators must keep pace so that human rights are properly protected. Despite the few regulations surrounding law enforcement's use of AFR, legislation should require that public agencies rigorously review biometric technologies for privacy concerns [64].

6 Public enforcement authorities vis-à-vis private actors in deploying AFR: a theoretical analysis of social licence

AFR is being used in public spaces, not only by law enforcement agencies but also increasingly by the private sector. The surveillance leads to chilling effects on social interactions [65]. The lack of privacy protection has a negative influence on society. AFR redefines the architecture of the social world, which renders it necessary to ensure the respect of privacy in an evolving socio-technical system

[42]. A fundamental issue is whether AFR is socially preferable, even though the utilisation of AFR increases public safety and benefits law enforcement.

6.1 Social license and ethical commitment

AFR innovations need to be imbued with public values before being integrated into public life [66]. There is some justification for AFR to be used by law enforcement agencies in public spaces. The public would accept the AFR technology in circumstances where there are adequate safeguards in place as well as clear public interests. From Pew's survey, 56% of Americans trust law enforcement agencies to use AFR responsibly in terms of the societal acceptability of, and public attitudes to, AFR; a 59% majority of U.S. adults think it is acceptable for them to use AFR to assess potential security threats in public spaces [67]. Some level of public surveillance does not pose a challenge given that the functionality falls squarely within citizens' reasonable expectation of privacy.[44] As such, surveillance of this kind does not run afoul of international privacy rules [68]. In contrast, people are less trusting of private actors.

Private companies are spearheading a rollout of the controversial technology, which causes concerns about the commercialisation of private data. The use of AFR is experiencing a commercial race to the bottom, with tech companies forced to choose between social responsibility and market success [69]. Private entities can only get access to facial verification, provided they can demonstrate that its use is "strictly necessary and proportionate" and has a clear legal basis. Otherwise, their use of AFR would be unlikely to withstand a legal challenge. Given that protecting privacy is a widely shared social preference [70], rigorous assessments of AFR use should be undertaken in the context of public and private partnership (PPP).

6.2 Private actors' profit-maximisation, critics and assessment under public and private partnership (PPP)

Non-law enforcement AFR uses also raise some controversial inquiries [26], given their rapid development for commercial applications. This rapid expansion raises unprecedented concerns about the nature of privacy and surveillance. Private actors' direct access to increasingly large quantities of data may result in the amplification of harms. They are capable of tremendous sophistication in analysis and decision-making [5]. AFR use exposes consumers to the risk of their private information being shared with unintended recipients due to data breaches. This has profound consequences for privacy and data protection rights.

6.2.1 Public and private partnership (PPP) in the assessment implications for privacy

AFR should be deployed only after an adequate evaluation of its purpose, benefits and risks [71]. Using the technology for security and surveillance reasons, public

[44] *Carpenter v. United States* 138 S. Ct. 2206 (2018).

actors typically rely on private companies for procuring and deploying AFR. The former need to obtain all necessary information from the latter, and the PPPs that combine government and business data sets plausibly help improve system performance [5]. However, data-sharing of surveillance material not only increases the potential of privacy harms, but also blurs the public and private boundaries given the differentiated rationales behind their access [72]. It is important to design tailored impact assessment methods to appropriately evaluate all affected rights in a comprehensive manner, which is conducive to ensuring a fundamental rights-compliant application of AFR [9]. A fully-fledged analysis and assessment of this kind need to be put in place from the outset of AFR use.

6.2.2 Profit maximisation vis-à-vis privacy protection

The forces of capitalism continue to drive toward greater profit despite the social implications of AFR. Businesses harness AI capabilities to improve analytic processing [39]. AFR-driven data analysis can provide a valuable assessment, i.e. consumer behavioural insights, which reflects consumer evidence-based decision-making [73]. This allows for a competitive advantage to the data users in predicting consumers' actions [75]. Once data is retained it can be readily repurposed for profit [74]. The market for facial recognition is increasing, with large investments of up to $1.6 billion in start-ups from China [75]. Zuboff describes this process as "surveillance capitalism" where data extraction greatly diminishes the information costs of corporate actors, redistributing privacy rights away from consumers and towards corporate actors [76]. Companies attempt to exploit the perks of AFR for commercial purposes, such as Alibaba trying to make "smile to pay" happen [77]. The asymmetric power over information between private AFR users and data subjects increases the potential for abuse. Out of a profit-maximising motive, companies can effectively manipulate customers based on facial expressions. There is little justification and low public approval for the use of AFR systems operated by a private actor. Only around 9% of UK residents approved of specific uses of AFR with appropriate safeguards [15].

6.2.3 Nurturing resilience in response to the emerging challenges

Companies are supposed to abide by the principles of legality, legitimacy and necessity. When collecting and processing personal information, they should clearly indicate the purpose, method and scope, and obtain the consent of the data subjects in advance [78]. In June 2019, Microsoft deleted a massive online data set that contained more than 10 million images of 100,000 individuals that was used to train other companies' AFR systems [79]. Ultimately, the company does not have a legal basis to process facial data under Article 9 of GDPR. Facebook paid five billion US$ to settle Federal Trade Commission (FTC) charges that the company violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information [80]. The unprecedented penalty should have the strongest possible deterrent effect in order to change Facebook's privacy culture to decrease the likelihood of continued violations.

The above cases demonstrate how privacy value has been maintained from both public enforcement and Microsoft's self-remedial measure. This should facilitate the transformation to integrate a built-in clause, that is, fundamental rights considerations need to be built into technical specifications, deployments and even contracts [9]. For instance, the EU Public Procurement Directive (2014/24/EU) strengthened EU Member States' commitment to socially responsible public procurement when purchasing a product or a service. Likewise, the EU could apply a similar approach when procuring the technology or commissioning innovative AFR-oriented research. A clear framework of AFR is needed to regulate how it can be used in both public and private spheres. The AFR-specific legislation is of great significance to promote human rights in the context of this emerging technology. It is imperative to put into place an effective set of laws and guidelines as the use of AFR proliferates. From the above-mentioned remarks, it is apparent that the legislative and judicial branches have been adapting the law to AFR to ensure that the proper balance is maintained between security and privacy [81]. However, the legal landscape is far from settled. The current framework does not keep pace with emerging technologies. Law is slow to protect personal privacy and individual liberty in the face of rapidly accelerating technologies of social control [26].

7 A paradoxical game in surveillance and data collection

The scope of surveillance capacities continues to grow [82]. Not all systems focus on database matching—some systems assess aggregate demographic trends or conduct broader sentiment analysis via facial recognition crowd scanning [39]. AFR can identify a person in a crowd in real time as well as track their movements, detect emotions and predict behaviour. A long-standing debate remains unaddressed as to whether the West still claims superiority in this scenario, which renders it important to ascertain the divergences between approaches.

7.1 A paradoxical debate in ethics and morality

AFR invokes substantial criticism in terms of the ethics and legality of its application. Questions on the role of law and ethics in governing AFR are more relevant than ever [83]. Turning the human face into another object for measurement and categorisation by companies touches the right to human dignity [84]. Given the users' strong moral and ethical obligation to ensure effective protection of privacy, the benefits of AFR must be weighed against the possible adverse effects it may have on subjects' privacy [85]. The implementation of AFR should ensure that its risks are not disproportionately borne by, or the benefits disproportionately flow to, a particular group [86]. In social psychology, moral realism is always behind a shadow that inhibits trade-offs and the achievement of compromise [87]. It is hardly justified to convert the question into a debate on whether economic well-being matters more or less than the human rights, like privacy [88]. In terms of the delicate conversion, of necessity is to differentiate their dimensionality with the two subjects evaluated.

AFR raises a host of ethical and legal questions about privacy along with surveillance. A classic question arises as to whether the benefits outweigh the intrusion into people's privacy, or more specifically, whether it is worth sacrificing privacy and civil liberties. The proposition *per se* is questionable given that it is on the ground of an incomplete hypothesis. Some fundamental variables must not be left out, like the diverse values and traditions. It is often difficult to harmonise diverse values when society develops public policy or weighs the costs and benefits of choices [89]. It has even been argued that AFR should be banned outright. As Axon's independent ethics board stated: "face recognition technology is not currently reliable enough to ethically justify its use" [90]. A consensus can hardly be established on ethical behaviour particularly between a competing set of ethical and policy priorities. Different countries are developing different regulatory regimes. Ethical principles can be used to inform deployments and frame policymaking. The absence of a binding code and national guidelines gives rise to inconsistent approaches. The absence of such framing has led to a widespread culture of disregard of the law and put privacy in danger [91]. As such, values, ethics or human rights should be embedded in those entities that profit from marketing surveillance capabilities [92]. However, building ethical AFR is an enormously complex undertaking.

7.2 Moral superiority vis-à-vis moral inferiority in the context of AFR

A key question is whether there are emerging threats of AFR-driven authoritarianism against democratic values, or whether there is no substantive difference in the deployment of AFR between the two [93]. As discussed above, AFR is being used in both the UK and China roughly in the same way, playing nearly the same roles in both public and private sectors. The classic debate is whether the UK or the West could claim moral supremacy over China in surveillance scenarios.

7.2.1 The driving force of digital capitalism and security

Data is the fuel that drives the AI engine [5]. Opening access to data will help gain insights that will transform the economy [94]. How to approach with surveillance largely determines whether the industry or even the state will be put at a competitive advantage in the current fierce digital competition [95]. The digital rights model has every relevance to corporate losses or gains. Limitations on data processing and resale curb corporate profits [96]. The tougher the privacy laws in the West, the less data there are, but data constitute the indispensable raw materials for AI. As West and Allen noted:

> Almost all the data are proprietary in nature and not shared very broadly with the research community, and this limits innovation and system design [5].

By taking a restrictive stance on issues of data collection and analysis, the West, particularly the EU, is putting its manufacturers and software designers at a significant disadvantage to the rest of the world [5]. Entrepreneurship and innovation is harmed, given that individuals will avoid "experimenting with new, controversial, or

deviant ideas" [97]. It makes more sense to think about the broad objectives desired in AI and enact policies that advance them.

The Chinese perception of privacy differs from that of the West. People's rights in privacy are less robust than those of their Western counterparts. China's cultural attitudes towards data and privacy norms are strikingly looser than those in the West [98]. In China, companies already have "considerable resources and access to voices, faces and other biometric data in vast quantities, which would help them develop their technologies" [99]. As a world-leading AI-powered surveillance state, China has embraced AFR, using it to implement a national surveillance system. The AFR-based surveillance capabilities have been on full display, which helps advance China's architecture for social control [93]. Surveillance is becoming pervasive, and algorithms score Chinese citizens on their behaviour. China has led the way in developing and deploying AFR, and set up the world's most sophisticated surveillance state. AFR could be used to prosecute minor crimes such as jaywalking or littering, and even allow the creation of a full "social credit" system of government surveillance [100]. The issue has been heightened by the growing use of the technology in China as part of a compulsory National Social Ratings and Surveillance Scheme [101]. As such, China makes it more permissive for companies so as not to hinder the development of AI.

China has been making a sustained effort for leadership and primacy [102]. As part of its push to advance its high-tech strategies, the country has been pushing forward its *Next Generation Artificial Intelligence Initiative* [103]. The State Council, China's highest administrative organs, launched the *Next Generation Artificial Intelligence Development Plan* in mid-2017, outlining a national ambition to become a leading AI power by 2030 [104]. Problematically, algorithms can identify faces but do so in ways that threaten privacy. The call for privacy could become a major challenge to China's internet titans, and eventually to the cyber-authoritarian aspirations of the Chinese government itself [56]. For the sake of substantial economic, social and strategic benefits, Chinese companies have been exporting the AFR-related products to like-minded governments in order to spread influence and promote an alternative governance model [105, 106]. As such, elements of China's model of surveillance inspire other autocracies [62]. Some critics have accused China and the surveillance companies of "exporting authoritarianism" via the technology [107].

As a polarising topic, AFR is sometimes seen as a problematic development in surveillance capitalism [108]. Despite the impact on privacy, this provides Chinese companies that have shaped standards an advantage in breaking into new potential markets [109]. It represents a smart short-cut for China to leverage global governance as well as businesses in AFR. China accounted for nearly half of the global facial recognition business in 2018 [109]. The market for facial recognition has grown 20% annually over the past 3 years and will be worth $9bn by 2022 [110]. While domestic concerns grow, China's facial recognition companies are leading the global market for public surveillance systems [111]. When there is a fundamental shift in the underlying balance of power, people's stance unconsciously falls into the trajectory of the Thucydidean rivalry between a rising China and the currently dominant West [112]. In the guise of ideological confrontations, conflicts will inevitably take place when a rising power threatens to displace a ruling one [113, 114].

7.3 Are there any hypothetical, ideological or substantive differences?

To pursue security, the West may have to collect data in order to safeguard themselves from cyber-attacks. France is the first EU country to use a nationwide facial recognition ID app [115]. Murgia and Yang argued that it is not a question of legality, but of morals and ethics in terms of the moral equivalence between China's authoritarianism and Western values [109]. However, in response to challenges posed by AFR, a perception of China's moral inferiority could be arguably a pseudo-proposition. It might well be worth referring to the famous Tacitus Trap, which contributes to the adoption of an absolutist moral stance that: 'when a government loses credibility, whether it tells the truth or a lie, to do good or bad, will be considered a lie or to do bad'.[45] As discussed in *Bridges*, the development and application of AFR by some police forces encapsulates a number of the problems that have arisen due to the lack of a clear legislative framework for the technology [20]. Both the UK and China are using increasingly sophisticated technology in their pervasive surveillance systems. In this scenario, the two countries are morally equivalent. It is simply difficult for the West to give up the moral superiority that underlies so much Western rhetoric about China [116]. One may argue for the UK's moral superiority because of its robust rights of privacy and free expression. However, Professor Paul Wiles, the UK's Biometrics Commissioner, notes that: "the technology is being rolled out in a 'chaotic' fashion in the absence of any clear laws" [117]. Despite the fact that China's public and private sectors have been aggressively using AFR,[46] the above argument also applies squarely to Western private entities. Companies based in liberal democracies are also actively selling sophisticated equipment [118]. To provide more in-depth demographics, Intel and Tencent try collaboratively to "gain new insights about their customers to both elevate the users' experience and drive business transformation" [119]. Along with Huawei, Google, BAE, NEC, Amazon and Alibaba are all involved in helping Saudi Arabia build AFR as well as other mass surveillance systems [120]. Some commentators observed:

> While debate over the use of facial recognition in the EU and the U.S. is focused on the privacy threat of governments or companies identifying and tracking people, the debate in China is often framed around the threat of leaks to third parties, rather than abuses by the operators themselves [107].

In this regard, moral or ethical issues have been complicated due largely to the Western and Chinese actors' convergence in deploying AFR. The data collector must ensure that "appropriate safeguards" and "enforceable data subject rights and effective legal remedies are available".[47] To meet the above criteria, an assessment should be based on a review of a country's privacy laws as well as on its record on "the rule of law, respect for human rights and fundamental freedoms" [121, 122].

[45] Tacitus' Histories 1.7: "when a ruler once becomes unpopular, all his acts, be they good or bad, tell against him."

[46] A September 2018 survey by Deloitte found that the use of facial recognition in China had grown significantly from the previous year, from just 18% in 2017 up to 44%.

[47] GDPR 46 (1).

It is vital to place procedural safeguards on AFR, such as requiring warrants and limiting the duration of surveillance, and alleviate concerns over security and privacy while encouraging innovation [123].

7.3.1 Standard: at stake is who will reshape future rules

China's individual data rights framework has profound global implications [124]. It increasingly seeks to influence internet governance and the information ecosystem [125]. The Chinese approach to data governance will play an important role in shaping global markets, technology development and policy. Its efforts to pioneer standards is a reflection of how the Chinese companies are seeking to supply surveillance technology across the world [126]. The AI Global Surveillance Index (AGSI) identifies that at least 64 countries have been actively incorporating AFR in their surveillance programs [39]. There is a first-mover advantage for whoever writes the new rules for the digital economy, and such an advantage in setting standards and rules can give a powerful edge to companies and businesses [109]. Dominant in the global facial recognition market, Chinese companies have made every submission to the UN for international standards on surveillance technology in the past 3 years [126]. The UN's International Telecommunication Union (ITU), which establishes common global specifications for technology, has received 20 standards proposals since 2016 from Chinese companies, including Huawei. Many of the submitted standards have already been approved, even though concerns are rising about how Chinese companies are gaining access to the personal data of individuals around the world [127].

8 Embed principles and rules into the AFR governance regime

AFR use has been operating in a legal vacuum [128]. The current legal landscape is fragmented. Neither a specific legal framework nor overarching principles of data protection are set at the global level to govern the deployment of AFR. This inadequate legal framework negatively impacts the foreseeability and accessibility of AFR policy. To fill the legal vacuum and develop an effective and cohesive future policy strategy, a proper governance framework that is fit for these emerging technologies in order to balance policing effectiveness and privacy is needed. The risk of interferences with fundamental rights is higher and therefore the necessity and proportionality test must be stricter [9]. The fundamental rights implications of using AFR vary considerably depending on the purpose, context and scope of the use [9]. It is essential to embed some principles to properly protect privacy while making efficient use of AFR. At stake in procedural control is the attachment of adequate balances and checks in the processing of AFR-driven data.

8.1 Enhance global governance by creating rules with teeth

The line between permissible and impermissible levels of surveillance is always blurred, which renders it imperative to protect the public interest through an AFR-based stringent regulation.

Meanwhile, providers must be accountable for ensuring that they do not facilitate human rights abuses. International law affirms its commitment to protecting privacy as a fundamental right. The Universal Declaration of Human Rights (UDHR) states that "no one shall be subjected to arbitrary interference with his privacy".[48] The right to privacy is also internationally recognised in the International Covenant on Civil and Political Rights (ICCPR).[49] Privacy is universally accepted at the international level and codified in the ICCPR, which states that: "[*n*]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence".[50] Although China is not a party to the Covenant, it is worth examining whether such pervasive surveillance implicates the ICCPR. The ICCPR privacy provision may not have enough teeth to offer a shield against Chinese-level facial surveillance.

Nevertheless, there are no uniform standards in terms of data access, data sharing or data protection [5]. The use of AFR is subject to insufficient regulation that is specifically designed to protect human rights given the new challenges posed by emerging technology [41]. There are no international rules that require law enforcement or companies to notify the people that an AFR system is in operation. Few rules govern access to and use of image databases. For instance, it remains unclear whether misuse of police data should be a criminal offence for which people are punished [129]. The absence of a comprehensive global governance framework to oversee AFR deployment has considerable implications for the protection of privacy. Substantial uncertainties and paramount challenges may lead to a global dialogue and the formation of a global practice on this critical issue, avoiding a potentially fractured global legal landscape [57].

There are clear advantages to having open norm-setting venues that aim to address AFR governance. AFR-specific regulation is necessary to account for the unique risks the technology poses for human rights [42]. Legislators should pass laws to regulate both public enforcement and private deployment via face recognition. Given the novelty of the technology as well as the lack of safeguard measures, global regulations must be created to avoid the violation of privacy in the digital age [130]. There is considerable need for a normative framework for AFR to help determine whether or not a specific deployment of AFR is human rights compliant [131]. The algorithms of the law must keep pace with new and emerging technologies.[51] Global safeguards and norms need to be instituted to shape how public and private actors use AFR [132]. In view of the above governance vacuum and institutional void, it is

[48] UDHR 1948 Art. 12.

[49] ICCPR Art. 17: (a) No one shall be subjected to arbitrary or unlawful interference with his privacy ...(b) Everyone has the right to the protection of the law against such interference or attacks.

[50] ICCPR Art. 17 (1).

[51] *R (Bridges) v. Chief Constable of South Wales Police and Others* [2019] EWHC 2341 (Admin).

worth exploring how to regulate the controversial use of AFR by referring to some well-established principles.

8.2 The test of necessity and the balance of interests

The use of extensive surveillance powers is sometimes abusive. Investigative AFR presents a unique analytical problem and requires a sophisticated balancing of interests [26]. The use of AFR is permissible only when it is being employed in the public interest. The issue about the proper balance between privacy and security has long been debated in public discourse as well in judicial arenas [133]. This might be straightforward in certain scenarios where there is a public interest in being able to identify those engaged in criminal activity [134]. Nevertheless, an objective of general interest, such as crime prevention or public security, is not *per se* sufficient to justify an interference [135]. Any interference with a right needs to be examined as to whether the given legitimate aim could not be obtained by other means that interfere less with the right guaranteed [136]. The GDPR introduces a data minimisation principle whereby personal data can be collected "limited to what is necessary in relation to the purposes for which they are processed".[52]

When determining whether a measure is necessary in a democratic society, an effective and targeted system should strike a balance between values, such as public safety, data security and fundamental rights. With an array of competing goals considered, it is essential to ascertain through some precedents whether security might be worth sacrificing privacy for [137].

Article 9 under GDPR specifies circumstances where the collection of biometric data is necessary "for reasons of substantial public interest". Pursuant to the GDPR, the processing of biometric data is only allowed where processing is:

> Necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[53]

The ECtHR held in *S. and Marper v. United Kingdom* that states should "strike a right balance" between protecting fundamental rights and developing new technologies.[54] In *Zakharov v. Russia*, the ECtHR dealt with the secret interception of mobile phone communications. It interpreted the principle of necessity that:

> As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim ... when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right

[52] GDPR 5(1)(c).

[53] GDPR Art. 9(2)(g).

[54] *S. and Marper v. the United Kingdom* (Nos. 30562/04 and 30566/04, ECtHR Grand Chamber 4 December 2008) §112.

> to respect for his or her private life ....The Court has to determine whether the procedures for implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society".[55]

In a landmark battle against UK mass surveillance, the ECtHR held that "the UK's regime for authorising bulk interception was incapable of keeping the 'interference' to what is 'necessary in a democratic society'."[56] The rulings represent a significant step forward in the protection of privacy. In the UK Supreme Court Case *Bank Mellat v. Her Majesty's Treasury*, Lord Reed formulated an applicable test for legality and necessity:

> (1) Whether the objective of the measure is sufficiently important to justify the limitation of a protected right
> (2) Whether the measure is rationally connected to the objective
> (3) Whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective
> (4) Whether, balancing the severity of the measure's effects on the rights of the persons to whom it applies against the importance of the objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter.[57]

The parameters improve greatly operationality of legal enforcement. The benefits have to be sufficiently great so as to justify any interference with other rights. Legislation should balance the competing needs of law enforcement with the fundamental protection of individual privacy [26]. The debate about the proper balance between privacy and public safety will continue to play out in the courts [4]. Apart from the key element of necessity, the use of AFR should also meet a proportionality requirement. It can be permissible only if the benefits are proportionate to any loss of liberty and privacy.

8.3 The test of proportionality

The appropriate extent of transparency or surveillance would be a dystopia [95]. The interference that needs to correspond to a pressing social need must be proportionate [138]. It will depend on the purpose for which AFR is used and on the safeguards in place to protect individuals from negative consequences. The proportionate use of AFR suggests that its application must be clearly warranted in existing laws [139]. The UK Surveillance Camera Code of Practice 2013 requires any police use of facial recognition or other biometric characteristic recognition systems to be clearly

[55] *Zakharov v. Russia* (Case No. 47143/06, ECtHR Grand Chamber, 4 December 2015).

[56] *Big Brother Watch & Others v. The United Kingdom* (Nos. 58170/13, 62322/14 and 24960/15, ECtHR, 13 September 2018).

[57] *Bank Mellat v. Her Majesty's Treasury* (201y [2013] UKSC 38 & [2013] UKSC 39).

justified and proportionate to meeting the stated purpose.[58] The UK's Human Rights Act 1998 requires that any interference with the ECHR Article 8 right to a private life be both necessary and proportionate. The Law Enforcement Directive (LED) lays down similar, albeit somewhat more permissive conditions,[59] which influences the regulation of AFR:

> The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage.[60]

The court considers how to apply the principle of proportionality in a variety of circumstances. When developing the rules and regulations that must ensure citizens' privacy protections, the judges undertake proportionality assessments. There are some rulings pertinent to the controversial issue.

In *Murray v. The United Kingdom*, the ECtHR found that the taking and retention of a photograph of a suspected terrorist without his/her consent was not disproportionate to the legitimate terrorist-prevention aims of a democratic society.[61] The principle articulated in *Murray* interprets the extent to which enforcement authorities make efforts to achieve the legitimate terrorism-prevention aims of a democratic sociality. The ruling is in line with the ECHR, which provides that "it is not intended to bar lawful and proportionate law enforcement activities".[62] In *Tele2 Sverige AB*, the Court of European Justice (CJEU) found the retention of communications data to be subject both to the requirements of Article 7 and Article 8 and a balancing test.[63] The CJEU further held: "the obligation to retain communications data must be proportionate, within a democratic society, to the objective of fighting serious crime ...".[64] These decisions sketch out the parameters within which any regulations of AFR will be evaluated, especially considering that the UK plans to remain a party to the ECHR after Brexit. To enable an informed assessment of the necessity and proportionality of AFR use, the more intrusive the technology is, the stricter the test must be [9]. Balances and checks need to be implemented to ensure that AFR is socially and lawfully used.

[58] *The Surveillance Camera Code of Practice* 2013 §3.2.3 "Any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose and be suitably validated. It should always involve human intervention before decisions are taken that affect an individual adversely".

[59] EU Law Enforcement Directive (LED) EU Directive 2016/680 Art. 10.

[60] EU Law Enforcement Directive (LED) EU Directive 2016/680 Recital 51.

[61] *Murray v. The United Kingdom* (No. 14310/88, ECtHR, Strasbourg, 28 October 1994).

[62] ECHR Art. 8(1).

[63] *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Watson and others* (CJEU, Joined Cases C-203/15 and C-698/15, 2016).

[64] *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Watson and others* (CJEU, Joined Cases C-203/15 and C-698/15, 2016).

8.4 Balances and checks in place for reasonable control

The balance and checks ensure that the crime-fighting benefits are counter-balanced with due regard to concerns about its impact on privacy and the current limitations of the algorithms it employs [140]. The right to an effective judicial remedy must be taken into account in relation to decisions by the users as well as the supervisory authority. Failing to address the legislative vacuum around new biometrics would put privacy in jeopardy. Harrell's challenge of the vacuum of legal checks and balances revealed a "surveillance-first, ask-permission-later system" [141]. One could argue that the exploitation of AFR presents a chilling model for fellow autocrats and poses a direct threat to open democratic societies [39]. It is imperative to maintain checks and balances and set rules to restrain those who collect and process biometric data.

8.4.1 Efficient safeguard and remedial measures

Of the utmost importance is to establish strong legal safeguards that guarantee privacy and accountability. Efficient institutions need to be put in place to ensure the efficacy of a mechanism to hold those actors accountable for their failure to abide by these principles. Potential rights-harming outcomes should be identified, and effective action taken to prevent and mitigate harms [142]. Both Article 32 of the GDPR and Article 29 of the LED require that Member States take necessary measures to prevent personal data from being disclosed to unauthorised parties. Such measures need to be integrated into a safeguards regime to protect the rights of people concerned.[65] Another pillar is that data subjects have the right to an effective remedy in case their rights are unduly violated. Such a right is well enshrined in the EU Charter of Fundamental Rights.[66] The access to remedy is also echoed in the GDPR, ensuring that a victim will have a channel for justice, which provides that:

> A controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[67]

These measures need to be conducted based on sophisticated privacy impact assessments.[68] Apparently, the existing protections are inadequate to guard against abuse. Merely setting up the mechanism of safeguards and accountability is not sufficient. It matters as to how the institution functions. Furthermore, it may need to include a private right of action to enhance deterrence against violation of privacy. While restrictions are made on the basis of the above principles, it is similarly essential to guarantee transparency and due process. There would be little sense if the users of AFR turned them into merely a box-ticking practice.

[65] Law Enforcement Directive Art. 20 (1); GDPR Art. 25 (1).

[66] EU Charter of Fundamental Rights Art. 47.

[67] GDPR Art. 46 (1).

[68] M-03-22, Office of Management and Budget (OMB) Guidance for Implementing the Privacy Provisions of the EGovernment Act of 2002 (26 September 2003).

Given the lack of adequate governance of AFR deployment [143], the related oversight is not sufficiently robust to protect against abuse.[69] As such, ethical design serves as a bulwark against the relentless pursuit of profit and power [144]. Since the government plays a dual role of player and referee in deploying AFR, an independent oversight authority becomes indispensable to keeping the controller and processor more accountable. This approach is consistent with Article 8 of the Charter on the protection of personal data, which requires the oversight of data processing by an independent authority.[70] To prevent fundamental rights violations, oversight authorities must have sufficient powers, resources and expertise [9]. The institutional approach helps to build trustworthiness through system validation by third parties.

8.4.2 Multi-stakeholder initiatives to develop best practices

The use of AFR raises a number of ethical issues and trade-offs, from concerns around privacy to a legitimate interest in public safety, which can only be resolved in public discourse [42]. Mere legal governance solutions are limited, suffering from conceptual ambiguity and lack of enforcement mechanisms [70]. It is important to go beyond conventional rhetoric to formulate and embed those fundamental values, like privacy initially. Of similar importance is to ensure that there is equitable stakeholder representation when developing AFR governance regimes [83]. There should be consensus on how to best balance AFR adoption between privacy and public interests [64]. More proactive approaches help to develop effective ways to raise public awareness for the trade-off between benefits and risks of its applications. Both the government and business focus more on economic growth, which could be at the expense of social inquiries. Initiating a much-needed and vigorous public debate about the proper balance between the AFR-related surveillance and privacy rights should be put high up on the agenda. Given the current limited role that civil society plays in shaping policies, the public should be afforded opportunities to voice concern and effectively object via democratic engagement [42]. The above proposals entail stronger procedural control regulating how law enforcement agencies and private companies legitimately deploy AFR [145]. The approaches are complementary, and the measures should be characterised with transparency, accountability and the avoidance of abuse.

9 Conclusion

AFR compromises the inviolable essential core of privacy and poses serious threats to fundamental rights. There is a lack of well-defined regulations controlling the collection, use, dissemination and retention of biometric identifiers. In view of the *status quo* of AFR governance, neither the legislative nor the judicial branch is well equipped to adjust the balance between the values, like security and privacy. The existing laws that protect individual biometric data are not adequate to respond to

[69] *Big Brother Watch & Others v. The United Kingdom* (13 September 2018) §§ 346–347.

[70] Charter of Fundamental Rights of the European Union Art. 8 (3).

the challenges posed by AFR. The deployment of such ground-breaking technology in the absence of a sufficient legal framework has resulted in complex ethical and legal repercussions. The use of AFR calls for a new legal and regulatory framework to avoid a dystopian future. The algorithms of the law must keep pace with new and emerging technologies. It will be up to the courts and policymakers to strike the right balance between the need for information and the right to privacy. Enforcement authorities must be ensured of being able to make efficient use of AFR's powerful investigatory roles, while privacy should be taken into reasonable account. The international community needs to develop a viable policy framework that ensures the respect of the above-mentioned privacy principles. More factors need to be considered, including the legal basis, necessity, proportionality and justification, in order to address intrusive AFR processing. It is likewise important to build up the consensus on protecting privacy while still enabling law enforcement to make use of surveillance's tremendous investigatory and crime-fighting tools.

Furthermore, it still remains unclear how non-state actors are collecting and using their personal data. To ensure the respect of human rights in this new socio-technical context, both public and private actors need to be committed to striking the right balance when using AFR. It is crucial to remain critical of the underlying aims of AFR governance solutions as well as those collateral impacts, especially in terms of legitimising private sector-led practice. There is still a gap to fill with regard to incentivising private entities to behave in a socially responsible way, striking a balance between maximising profits and protecting fundamental rights. Impact assessments are important tools to comprehensively assess the risks involved in AFR. Given that processing of personal data constitutes a limitation of privacy, it needs to be subjected to a strict necessity and proportionality test, including a clear legal basis to do so and a legitimate aim pursued. To achieve this goal, efficient mechanisms of balances and checks are indispensable to ensure that the proposed test principles will function properly. Due to the lack of qualitative and quantitative analysis based on solid data, it takes time to optimise the roadmap of addressing the global challenge.

Funding Open access funding provided by University of Sussex.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Hirose M (2017) Privacy in public spaces: the reasonable expectation of privacy against the dragnet use of facial recognition technology. Conn Law Rev 49(5):1591
2. Borshoff I (2019) UK court backs police in facial recognition lawsuit. Politico

3. Rubinstein I (2018) Privacy localism. Wash Law Rev 93:1961–2049
4. Hamann K, Smith R (2019) Facial recognition technology: where will it take us? Crim Justice 34(1):9–13
5. West D, Allen J How artificial intelligence is transforming the world (Washington, DC., Brookings). https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/ (Created 24 Apr 2018). Accessed 1 Dec 2020
6. Jonathan Shaw, 'Artificial Intelligence and Ethics' Harvard Magazine (February 2019)
7. U.S. National Institute for Standards and Technology (NIST), NIST evaluation shows advance in face recognition software's capabilities. https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities (Created 30 Nov 2018). Accessed 17 Dec 2020
8. Deeks A, Togawa Mercer S (2018) Facial recognition software: costs and benefits. Lawfare
9. European Union Agency for Fundamental Rights Facial recognition technology: fundamental rights considerations in the context of law enforcement (Brussels, 2019). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf. Accessed 10 Dec 2020
10. Condliffe J (2017) Facial recognition is getting incredibly powerful-and ever more controversial. MIT Technol Rev
11. Tucker C (2019) Privacy, algorithms, and artificial intelligence. In: Agrawal AK, Gans J, Goldfarb A (eds) The economics of artificial intelligence: an agenda. University of Chicago Press, , pp 423–437
12. Acquisti A, Gross R, Stutzman F (2014) Face recognition and privacy in the age of augmented reality. J Priv Confident 6(2):1–20
13. Katz v. United States, 389 U.S. 347 (1967)
14. Rubinstein I, Nojeim G, Lee R (2014) Systematic government access to personal data: a comparative analysis. Int Data Priv Law 4(2):96–119
15. (2019) Beyond face value: public attitudes to facial recognition technology' (Ada Lovelace Institute). https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf (Created 09.2019). Accessed 21 Jan 2021
16. FRA (2018) Council of Europe and EDPS. In: Handbook on European data protection law. Publications Office, Luxembourg, pp 35–52
17. European Court of Human Rights (ECtHR) (2019) Guide on article 8 of the European convention on human rights-right to respect for private and family life, home and correspondence. Council of Europe, Strasbourg, p §§133
18. 'Perfected in China, A Threat in the West' Economist (2 June 2018)
19. Crawford K (2019) Halt the use of facial-recognition technology until it is regulated. Nature 572:565
20. House of Commons Science and Technology Committee (2019) The work of the biometrics commissioner and the forensic science regulator contents. House of Commons Science and Technology Committee, London (https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197003.htm)
21. Pugh A (2019) 'Facing off' Global Data Review (15. November)
22. Freiwald S, Métille S (2013) Reforming surveillance law: the Swiss model. Berkeley Technol Law J 28(2):1261–1332
23. Jonathan Day, 'Facial Recognition Surveillance a Threat to Law-Abiding Citizens' LibertiesEU (21 September 2018)
24. Mehreen Khan, 'EU Plans Sweeping Regulation of Facial Recognition' Financial Times (22 August 2019)
25. Garvie C, Bedoya A, Frankle J Unregulated police face recognition in America' (Georgetown law centre on privacy and technology). https://www.perpetuallineup.org/ (Created 18 Oct 2016). Accessed 30 Dec 2020
26. Guthrie Ferguson A Written testimony of professor Andrew Guthrie Ferguson before the house of representatives committee on oversight and reform-hearing on: facial recognition technology: (part 1) its impact on our civil rights and liberties. https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-FergusonA-20190522.pdf (Created 22 May 2019). Accessed 2 Feb 2021
27. Genie Gorbonosov, 'Patel v. Facebook: Ninth Circuit Grants Facebook's Motion to Stay in Facial Recognition Lawsuit' JOLT Digest (14 November 2019)
28. Ohm P (2019) The many revolutions of Carpenter. Harv J Law Technol 32(2):357–416
29. Dave Lee, 'San Francisco Is First US City to Ban Facial Recognition' BBC (15 May 2019)
30. Kari Paul, 'San Francisco Could Ban Government Agencies from Using Facial Recognition Technology' The Guardian (7 May 2019)

31. Kate Conger, Richard Fausset and Serge Kovaleski, 'San Francisco Bans Facial Recognition Technology' The New York Times (14 May 2019)
32. Schatz, blunt introduce bipartisan commercial facial recognition privacy act. https://www.schatz.senate.gov/press-releases/schatz-blunt-introduce-bipartisan-commercial-facial-recognition-privacy-act (Created 14 Mar 2019). Accessed 18 March 2021
33. Commercial Facial Recognition Privacy Act of 2019 (S. 847–116th Congress 1st Session)
34. Stephanie Hare, 'Facial Recognition is Now Rampant, The Implications for Our Freedom are Chilling' The Guardian (18 August 2019) "With more than 6 million CCTV cameras in the UK, and 420,000 in London."
35. David Davis, 'Facial Recognition Technology Threatens to End All Individual Privacy' Financial Times (20 September 2019)
36. Lizzie Dearden, 'Police Used Facial Recognition Technology Lawfully, High Court Rules in Landmark Challenge' The Independent (4 September 2019)
37. Stephen White, 'Regulator "Advocating a More Cautious Approach" to Facial Recognition Technology' PrivSec.Report (1 November 2019)
38. UK Biometrics Commissioner Automated facial recognition. https://www.gov.uk/government/news/automated-facial-recognition (Created 10 Sept 2019). Accessed 20 Feb 2021
39. Feldstein S 'the global expansion of AI surveillance' (Washington DC, carnegie endowment for international peace). https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 (Created 17 Sept 2019). Accessed 4 Dec 2020
40. UK Parliament (2019) Issues with biometrics and forensics significant risk to effective functioning of the criminal justice system
41. Olatokun M Automated facial recognition and the rule of law (London, BIICL). https://binghamcentre.biicl.org/comments/69/automated-facial-recognition-and-the-rule-of-law (Created 8 Oct 2019). Accessed 8 March 2021
42. Ruhrmann H (2019) Facing the future: protecting human rights in policy strategies for facial recognition technology in law enforcement-case studies from the United Kingdom and the United States' (the CITRIS policy lab). http://citris-uc.org/wp-content/uploads/2019/09/Facing-the-Future_Ruhrmann_CITRIS-Policy-Lab.pdf (Created 05.2019). Accessed 27 Dec 2020
43. Shannon Togawa Mercer and Ashley Deeks, 'One Nation Under CCTV': The UK Tackles Facial Recognition Technology' LawFare (7 May 2018)
44. (2013) Home Office, 'Surveillance Camera Code of Practice. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf. Accessed 19 Nov 2020
45. (2013) Home office, 'surveillance camera code of practice pursuant to section 29 of the protection of freedoms act 2012. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/157901/code-of-practice.pdf. Accessed 27 Jan 2021
46. Surveillance Camera Commissioner The police use of automated facial recognition technology with surveillance camera systems' section 33 protection of freedoms act 2012. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf (Created 03.2019). Accessed 1 Feb 2021
47. Ed Bridges, 'Facial Recognition Tech is Creeping into Our Lives' The Guardian (21 May 2019)
48. Lizzie DeardenHome, 'Facial Recognition Becoming 'Epidemic' in British Public Spaces' Independent (16 August 2019)
49. UK Parliament The work of the biometrics commissioner and the forensic science regulator. https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197002.htm (Created 18 July 2019). Accessed 16 Jan 2021
50. Yue Song, 'Hangzhou Safari Park's AFR Use without Consumers' Consent Was Unlawful' Xinhua News (23 November 2020)
51. Bing Guo v Hangzhou Safari Park (Hangzhou Fuyang District Curt, Zhejiang 0111, Civil No. 6971, 20 November 2020)
52. Shen Lu, 'Facial Recognition Is Running Amok in China. The People Are Pushing Back' Vice (10 December 2020)
53. Yuan Yang and Nian Liu, 'China Survey Shows High Concern over Facial Recognition Abuse' Financial Times (5 December 2019)
54. 'Facial Recognition Annual Report 2019' (Nandu Personal Information Protection Research Centre, 5 December 2019)

55. Billie Thomson, 'Concerns over Personal Data Security Soar in China after Tourist Waged War on Beijing's 'Big-Brother' Surveillance System because Zoo 'Forced Him to Use Facial-Recognition Cameras' Daily Mail (8 January 2020)
56. Paul Mozur, 'Internet Users in China Expect to Be Tracked. Now, They Want Privacy' The New York Times (4 January 2018)
57. Winston Ma, 'China Is Waking up to Data Protection and Privacy' Weforum (12 November 2019)
58. Samm Sacks, Qiheng Chen, and Graham Webster, 'China's Personal Information Security Specification' New America (8 February 2019)
59. Lee S Coming into focus: China's facial recognition regulations' (Washington DC, centre for strategic and international studies (CSIS)). https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations (Created 4 May 2020). Accessed 8 Feb 2021
60. Zhenhuan Ma, 'Park Alters Entry Rules Following Facial Fecognition Tech Lawsuit' China Daily (7 November 2019)
61. Sacks S, Xiaomeng L, Li M What the Facebook scandal means in a land without Facebook: a look at China's burgeoning data protection regime' (Washington, DC, center for strategic and international studies (CSIS). https://www.csis.org/analysis/what-facebook-scandal-means-land-without-facebook-look-chinas-burgeoning-data-protection (Created 25 Apr 2018). Accessed 31 Jan 2021
62. 'Does China's Digital Police State Have Echoes in the West?' Economist (31 May 2018)
63. Daniel Malan, 'The Law Can't Keep up with New Tech. Here's How to Close the Gap' World Economic Forum (21 Jun 2018)
64. Ringrose K (2019) Law enforcement's pairing of facial recognition technology with body-worn cameras escalates privacy concerns. Virginia Law Rev 105:57–66
65. Jonothan Penney (2016) Chilling effects: online surveillance and Wikipedia use. Berkeley Technol Law J 31:117–123
66. (2019) Beyond face value: public attitudes to facial recognition technology' (Ada Lovelace institute). https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf (Created 09.2019). Accessed 2 March 2021
67. Smith A More than half of U.S. adults trust law enforcement to use facial recognition responsibly' (Washington, DC, pew research center). https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/ (Created 5 Sept 2019). Accessed 1 Feb 2021
68. Ashley Deeks, 'China's Total Information Awareness: Second-Order Challenges' LawFare (16 January 2018)
69. Jay Greene and Douglas MacMillan, 'Microsoft Pushes Urgency of Regulating Facial Recognition Technology' Wall Street Journal (6 December 2018)
70. Welinder Y (2012) A face tells more than a thousand posts: developing face recognition privacy in social networks. Harv J Law Technol 26(1):165–239
71. EPIC complaint in re hireVue (Washington DC, federal trade commission (FTC). https://www.epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf (Created 6 Nov 2019). Accessed 15 Jan 2021
72. Wright E (2019) The future of facial recognition is not fully known: developing privacy and security regulatory mechanisms for facial recognition in the retail sector. Fordham Intellect Prop Media Entertain Law J 29(2):611–685
73. Peppet S (2014) Regulating the Internet of things: first steps toward managing discrimination, privacy, security, and consent. Tex Law Rev 93:85–90
74. Nicole Martin, "Was the Facebook '10 Year Challenge' A Way to Mine Data for Facial Recognition AI?" Forbes (17 January 2019)
75. Jamie Condliffe, 'Big Investors are Placing Bets on China's Facial Recognition Start-ups' The New York Times (24 July 2018)
76. Zuboff S (2015) Big other: surveillance capitalism and the prospects of an information civilization. J Inf Technol 30(1):75–83
77. Agence France-Presse, 'Smile-to-Pay: Chinese Shoppers Turn to Facial Payment Technology' Financial Times (4 September 2019)
78. de Hert P, Papakonstantinou V (2015) The data protection regime in China' (Brussels, European parliament). http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf (Created 10.2015). Accessed 30 Dec 2020
79. Victoria Petrock, 'Culture Clash on Facial Recognition: China and the West Take Different Paths' eMarketer (21 October 2019)
80. FTC (2019) FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook. FTC, Washington DC

81. Freiwald S, Smith SW (2018) The Carpenter chronicle: a near-perfect surveillance. Harv Law Rev 132:205–235
82. Keats Citron D, Gray D (2013) Addressing the Harm of total surveillance: a reply to professor Neil Richards. Harv Law Rev 126:262–274
83. Cath C (2018) Governing artificial intelligence: ethical, legal and technical opportunities and challenges. Philos Trans Royal Soc A 376(2133):1–8
84. Jakubowska E Facial recognition and fundamental rights 101' European digital rights. https://edri.org/facial-recognition-and-fundamental-rights-101/ (Created 4 Dec 2019). Accessed 27 Jan 2021
85. Anderson J, Rainie L, Luchsinger A Artificial intelligence and the future of humans (Washington DC, pew research centre). https://www.pewresearch.org/internet/2018/12/10/artificial-intelligence-and-the-future-of-humans/ (Created 10 Dec 2018). Accessed 29 Nov 2020
86. Introna L, Nissenbaum H (2009) Facial recognition technology: a survey of policy and implementation issues (New York university, report of the centre for catastrophe preparedness and response). https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf?. Accessed 13 Dec 2020
87. Pölzler T (2018) How to measure moral realism. RevPhilPsych 9:647–670
88. McCrudden C (2008) Human dignity and judicial interpretation of human rights. Eur J Int Law 19(4):655–724
89. Cuéllar M-F Reconciling law, ethics, and artificial intelligence: the difficult work ahead (Stanford, institute for human-centered AI). https://hai.stanford.edu/news/reconciling-law-ethics-and-artificial-intelligence-difficult-work-ahead (Created 5 Feb 2019). Accessed 24 Dec 2020
90. Charlie Warzel, 'A Major Police Body Cam Company Just Banned Facial Recognition' The New York Times, (27 June 2019)
91. Nemitz P (2018) Constitutional democracy and technology in the age of artificial intelligence. Philos Trans A 376(2133):1–14
92. Madhumita Murgia and Christian Shepherd, 'Western AI Researchers Partnered with Chinese Surveillance Firms' Financial Times (19 April 2019)
93. Polyakova A, Meserole C Exporting digital authoritarianism' brookings policy briefings (Washington DC, Brookings). https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf (Created 26 Aug 2019). Accessed 7 Jan 2021
94. Buck I Game changers: artificial intelligence part I-testimony before the house committee on oversight and government reform subcommittee on information technology (Washington DC). https://www.govinfo.gov/content/pkg/CHRG-115hhrg30296/html/CHRG-115hhrg30296.htm (Created 14 Feb 2018). Accessed 1 March 2021
95. Henry Mance, 'Is Privacy Dead?' Financial Times (19 July 2019)
96. Calo R (2014) Digital market manipulation. George Wash Law Rev 82:995–1031
97. Richards N (2013) The dangers of surveillance. Harv Law Rev 126:1934–1965
98. Stephany Zoo, 'What Africa Can Learn from China about Data Privacy' World Economic Forum (26 June 2019)
99. Paul Mozur and Keith Bradsher, 'China's A.I. Advances Help Its Tech Industry, and State Security' New York Times (3 December 2017)
100. Paul Karp, 'Dutton's Home Affairs Department Argues against Restrictions on Facial Recognition' The Guardian (3 May 2018)
101. Shannon Bond, 'Inside China's Surveillance State' Financial Times (19 July 2018)
102. Ding J (2018) Deciphering China's AI dream (future of humanity institute, university of Oxford). https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf. Accessed 8 Feb 2021
103. Hass R, Balin Z (2019) US-China relations in the age of artificial intelligence' Brookings (Washington, DC., the Brookings institution). https://www.brookings.edu/research/us-china-relations-in-the-age-of-artificial-intelligence/ (Created 19 Jan 2019). Accessed 28 Feb 2021
104. O'Meara S (2019) Will China lead the world in AI by 2030? Nature 572:427–428
105. U.S. House of Representatives, Permanent Select Committee on Intelligence Hearing 'China's digital authoritarianism: surveillance, influence, and political control. https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=109462 (Created 16 May 2019). Accessed 18 Feb 2021
106. Elias Biryabarema, 'Uganda's Cash-Strapped Cops Spend $126 Million on CCTV from Huawei' Reuters (16 August 2019)
107. Yuan Yang and Madhumita Murgia 'Facial Recognition: How China Cornered the Surveillance Market' Financial Times (6 December 2019)
108. Göran Wågström, 'The Dangers of Facial Recognition' Forbes (24 October 2019)

109. Alan Beattie, 'Technology: How the US, EU and China Compete to Set Industry Standards' Financial Times (24 July 2019)
110. Madhumita Murgia, 'Who's Using Your Face? The Ugly Truth about Facial Recognition' Financial Times (18 September 2019)
111. Yuan Yang and Nian Liu, 'China Survey Shows High Concern over Facial Recognition' Financial Times (5 December 2019)
112. Gideon Rachman, 'Year in a Word: Thucydides's Trap' Financial Times (19 December 2018)
113. Kello L (2017) The virtual weapon and international order. Yale University Press, New Haven
114. Graham Allison, 'Review: An Uneasy Unpeace' The Wall Street Journal (21 January 2018)
115. Henry Samuel, 'France to become first EU country to use nationwide facial recognition ID App' Telegraph (3 October 2019)
116. Andrew Keane Woods, 'China and the Hypocrisy of American Speech Imperialism' Lawfare (18 October 2019)
117. Hannah Devlin, "'We are Hurtling towards a Surveillance State': The Rise of Facial Recognition Technology" The Guardian (5 October 2019)
118. Ryan Tracy, 'World Catching up with China on Surveillance Tech' The Wall Street Journal (17 September 2019)
119. Jonathan Chadwick, "Tencent Teams up with Intel for Retail Surveillance Camera and "AI Box"" Computer Business Review (2 November 2018)
120. Rob Evans, "BAE 'Secretly Sold Mass Surveillance Technology to Repressive Regimes" Guardian (14 June 2017)
121. Office of the United Nations High Commissioner for Human Rights (2014) The right to privacy in the digital age. Human Rights Council 27th Session Agenda items 2 and 3, 30 June 2014
122. Mistale Taylor (2015) The EU's human rights obligations in relation to its data protection laws with extraterritorial effect. Int Data Priv Law 5(4):246–256
123. Chris Coons, Mike Lee, et al., "How to Build Guardrails for Facial Recognition Technology" Brookings (5 December 2019)
124. Lorand Laskai, Segal A The encryption debate in China" international encryption brief (Washington DC, carnegie endowment for international peace. https://carnegieendowment.org/2019/05/30/encryption-debate-in-china-pub-79216. Accessed 30 May 2019
125. Digital surveillance unleashed: implications for human rights, democracy, and American influence" (Washington, DC, centre for strategic and international studies (CSIS). https://www.csis.org/events/digital-surveillance-unleashed-implications-human-rights-democracy-and-american-influence (Created 13 Feb 2019). Accessed 5 Dec 2020
126. Anna Gross and Madhumita Murgia, "China Shows its Dominance in Surveillance Technology" Financial Times (27 December 2019)
127. Oliver Smith, "Chinese Tech Groups Shaping UN Facial Recognition Standards" Financial Times (1 December 2019)
128. Purshouse J, Campbell L (2019) Privacy, crime control and police use of automated facial recognition technology. Crim Law Rev 3(188):204
129. "Does China's Digital Police State Have Echoes in the West?" Economist (2 June 2018)
130. UNHRC (2018) The right to privacy in the digital age-Report of the United Nations High Commissioner for Human Rights. Human Rights Council, 39th Session, Agenda Items 2 & 3, 3 Aug 2018
131. McGregor L, Daragh M, Ng V (2019) International human rights law as a framework for algorithmic accountability. Int Comp Law Q 68(2):309–343
132. Stanton C (2019) San Francisco is the first city in the world to restrict government use of facial recognition technology. Hopefully It's Not the Last." Techdirt, 17 May 2019
133. Neil Desai, "If we are to meet the enormous challenge of balancing security and privacy, all stakeholders must come together for a public debate on the subject." Policy Options (19 July 2017)
134. Hallowell N, Amoore L et al Ethical issues arising from the police use of live facial recognition technology" (interim report of the biometrics and forensics ethics group facial recognition working group. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf (Created 02.2019). Accessed 26 Jan 2021
135. The Crown Prosecution Service (CPS), Human rights and criminal prosecutions: general principles. https://www.cps.gov.uk/legal-guidance/human-rights-and-criminal-prosecutions-general-principles (Created 18 Sept 2019). Accessed 23 Jan 2021

136. CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (8 April 2014)
137. Acquisti A, John LK, Loewenstein G (2013) What is privacy worth? J Leg Stud 42:249–274
138. Janneke Gerards (2013) How to improve the necessity test of the European court of human rights. Int J Const Law 11(2):466–490
139. European Commission (2019) Independent high-level expert group on artificial intelligence-ethics guidelines for trustworthy on AI, pp 33–34
140. Drury M, Hayes J Privacy: proceed with caution—the ICO opinion of facial recognition technology. https://gdpr.report/news/2019/12/24/privacy-proceed-with-caution-the-ico-opinion-of-facial-recognition-technology-2/ (Created 24 Dec 2019). Accessed 1 Nov 2020
141. Drew Harrell, "FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches" Washington Post (7 July 2019)
142. Turner Lee N, Resnick P, Barton G Algorithmic bias detection and mitigation: best practices and policies to reduce consumer harms" (Washington DC, Brookings). https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/ (Created 22 May 2019). Accessed 28 Dec 2020
143. Mann M, Smith M (2017) Automated facial recognition technology: recent developments and approaches to oversight. UNSW Law J 40(1):121–145
144. Lizzie O'Shea, "Tech Has No Moral Code. It Is Everyone's Job Now to Fight for One" The Guardian (25 April 2018)
145. Arthur Piper, "Automated Facial Recognition Technology Comes of Age" IBA Global Insight (September 2019)